

CLAIMS

What is claimed is:

- 1 1. A system for analyzing a network, scanning the network, and detecting
2 intrusions in the network, comprising:
 - 3 (a) a plurality of agents coupled to a plurality of computers interconnected via a
4 network, each agent adapted to collect information;
 - 5 (b) a plurality of host controllers coupled to the agents for collecting the information
6 from the agents, scanning the information, and detecting intrusions in the
7 network; and
 - 8 (c) a plurality of zone controllers coupled to the host controllers for analyzing an
9 output of the host controllers, and executing security actions in response thereto.
- 1 2. The system as recited in claim 1, wherein the host controllers are further capable
2 of cybercop services.
- 1 3. The system as recited in claim 1, wherein the zone controllers are further capable
2 of integrated reporting.
- 1 4. The system as recited in claim 1, wherein the host controllers and the zone
2 controllers operate based on business rules.
- 1 5. The system as recited in claim 1, wherein the business rules are user-
2 configurable.

- 1 6. A method for analyzing a network, scanning the network, and detecting
2 intrusions in the network, comprising:
- 3 (a) collecting information relating to a plurality of computers utilizing a plurality of
4 agents coupled to the computers via a network;
- 5 (b) collecting the information from the agents utilizing a plurality of host controllers
6 coupled to the agents;
- 7 (c) scanning the information utilizing the host controllers;
- 8 (d) detecting intrusions in the network utilizing the host controllers;
- 9 (e) collecting the information from the host controllers utilizing a plurality of zone
10 controllers coupled to the host controllers;
- 11 (f) analyzing output of (b)-(d) utilizing the zone controllers; and
- 12 (g) executing security actions based on the analysis utilizing the zone controllers.
- 1 7. The method as recited in claim 6, wherein the host controllers are further
2 capable of cybercop services.
- 1 8. The method as recited in claim 6, wherein the zone controllers are further
2 capable of integrated reporting.
- 1 9. The method as recited in claim 6, wherein the host controllers and the zone
2 controllers operate based on business rules.
- 1 10. The method as recited in claim 6, wherein the business rules are user-
2 configurable.
- 1 11. A computer program product for analyzing a network, scanning the network and
2 detecting intrusions in the network, comprising:

FOIA b 7 - D

- 3 (a) computer code for collecting information relating to a plurality of computers
- 4 utilizing a plurality of agents coupled to the computers via a network;
- 5 (b) computer code for collecting the information from the agents utilizing a plurality
- 6 of host controllers coupled to the agents;
- 7 (c) computer code for scanning the information utilizing the host controllers;
- 8 (d) computer code for detecting intrusions in the network utilizing the host
- 9 controllers;
- 10 (e) computer code for collecting the information from the host controllers utilizing a
- 11 plurality of zone controllers coupled to the host controllers;
- 12 (f) computer code for analyzing output of (b)-(d) utilizing the zone controllers; and
- 13 (g) computer code for executing security actions based on the analysis utilizing the
- 14 zone controllers.

1 12. The computer program product as recited in claim 11, wherein the host

2 controllers are further capable of cybercop services.

1 13. The computer program product as recited in claim 11, wherein the zone

2 controllers are further capable of integrated reporting.

1 14. The computer program product as recited in claim 11, wherein the host

2 controllers and the zone controllers operate based on business rules.

1 15. The computer program product as recited in claim 14, wherein the business rules

2 are user-configurable.

1 16. A system for analyzing a network, scanning the network and detecting intrusions

2 in the network, comprising:

- 3 (a) agent means adapted to collect information;

- 4 (b) host controller means for collecting the information from the agent means,
5 scanning the information, and detecting intrusions in the network; and
6 (c) zone controller means for analyzing an output of the host controller means, and
7 executing security actions in response thereto.

1 17. The system as recited in claim 16, wherein the host controller means is further
2 capable of cybercop services.

1 18. The system as recited in claim 16, wherein the zone controller means is further
2 capable of integrated reporting.

1 19. The system as recited in claim 16, wherein the host controller means and the
2 zone controller means operate based on business rules.

1 20. The system as recited in claim 19, wherein the business rules are user-
2 configurable.

1 21. A system for analyzing a network, scanning the network, and detecting
2 intrusions in the network, comprising:

- 3 (a) a plurality of agents coupled to a plurality of computers interconnected via a
4 network, each agent adapted to collect information;
5 (b) a plurality of host controllers coupled to the agents for collecting the information
6 from the agents;
7 (c) means for scanning the information;
8 (d) means for detecting intrusions in the network;
9 (e) a plurality of zone controllers coupled to the host controllers for analyzing an
10 output of the host controllers; and

11 (f) means for executing security actions in response to at least one of the scanning,
12 the detecting, and the analyzing.

1 22. A method for providing business rule-based network services utilizing a
2 network, comprising:

3 (a) collecting information relating to a plurality of computers utilizing a plurality of
4 agents coupled to the computers via a network;

5 (b) collecting the information from the agents utilizing a plurality of controllers
6 coupled to the agents;

7 (c) identifying a plurality of business rules; and

8 (d) providing services utilizing the information based on the business rules.

1 23. The method as recited in claim 22, wherein the services include analysis
2 services, intrusion detection services, anti-virus services, and security services.

1 24. The method as recited in claim 22, wherein the services include at least one of
2 analysis services, intrusion detection services, anti-virus services, and security
3 services.